WHAT IS CLAIMED IS:

1. A method comprising:

encrypting a plurality of non-volatile storage regions, each being encrypted using a different encryption key from a set of encryption keys;

making a first subset of the encryption keys available to a first user thereby granting the first user access to a corresponding first subset of non-volatile storage regions, the first subset of the encryption keys consisting of one, a plurality, or all of the encryption keys; and

making a second subset of the encryption keys available to a second user thereby granting the second user access to a corresponding second subset of non-volatile storage regions, the second subset consisting of one, a plurality, or all of the encryption keys.

2. The method of Claim 1, further comprising:

generating a first private-public encryption key pair and a second private-public encryption key pair;

making the first private key available only to the first user and the second private key only to the second user; and

encrypting the first subset of the encryption keys using the first public encryption key, and the second subset of the encryption keys using the second public encryption key.

3. The method of Claim 2, further comprising:

storing the first private key and the second private key in a secure memory unit;

protecting access to the first private key with a first authentication token, the first authentication token being known only to the first user; and

protecting access to the second private key with a second authentication token, the second authentication token being known only to the second user.

4. The method of Claim 3, further comprising:

requesting an authentication token from a user attempting to access one or more of the non-volatile storage regions;

authenticating the user, if the user's authentication token matches one of the authentication tokens used to protect access to one of the private keys;

decrypting, with the secure encryption module using the authenticated user's private key, a corresponding subset of encryption keys, in response to authenticating the user; and

decrypting a corresponding subset of non-volatile storage regions, thereby making the corresponding subset of non-volatile storage regions available to the authenticated user.

5. The method of Claim 3, wherein the authentication tokens are selected from the group consisting of: passwords, fingerprints signatures, voice signatures, retina signatures, and secure access devices.

6. The method of Claim 4, wherein the encrypting and decrypting the plurality of non-volatile storage regions are performed using full-disk encryption software.

7. The method of Claim 1, wherein one of the non-volatile storage regions is adapted to store an operating system and data common to the first user and to the second user.

8. The method of Claim 1, wherein one of the non-volatile storage regions is adapted to store user-specific data of the first user.

9. The method of Claim 1, wherein one of the non-volatile storage regions is adapted to store user-specific data of the second user.

10. The method of Claim 1, wherein the non-volatile storage regions are chosen from the group consisting of: volumes, disks, partitions, and folders/directories.

11. An apparatus comprising:

one or more processors;

a memory accessible by the one or more processors;

a plurality of non-volatile storage regions accessible by the one or more processors;

an encryption unit adapted to encrypt the plurality of non-volatile storage regions, each with a different encryption key selected from a set of encryption keys;

wherein a first subset of the encryption keys is made available to a first user thereby granting the first user access to a corresponding first subset of non-volatile storage regions, the first subset of the encryption keys consisting of one, a plurality, or all of the encryption keys; and

wherein a second subset of the encryption keys is made available to a second user thereby granting the second user access to a corresponding second subset of non-volatile storage regions, the second subset consisting of one, a plurality, or all of the encryption keys.

12. The apparatus of Claim 11, further comprising a secure encryption module adapted to:

generate a first private-public encryption key pair and a second private-public encryption key pair;

make the first private key available only to the first user and the second private key only to the second user; and

encrypt the first subset of the encryption keys using the first public encryption key, and the second subset of the encryption keys using the second public encryption key.

13. The apparatus of Claim 12, wherein the secure encryption module is further adapted to:

store the first private key and the second private key;

protect access to the first private key with a first authentication token, the first authentication token being known only to the first user; and protect access to the second private key with a second authentication token, the second authentication token being known only to the second user.

14. The apparatus of Claim 13,

wherein the secure encryption module is further adapted to:

request an authentication token from a user attempting to access one or more of the non-volatile storage regions,

authenticate the user, if the user's authentication token matches one of the authentication tokens used to protect access to one of the private keys, and

decrypt, using the authenticated user's private key, a corresponding subset of encryption keys, in response to authenticating the user, and

wherein the encryption unit is further adapted to decrypt a corresponding subset of non-volatile storage regions, thereby making the corresponding subset of non-volatile storage regions available to the authenticated user.

15. The apparatus of Claim 13, wherein the authentication tokens are selected from the group consisting of: passwords, fingerprints signatures, voice signatures, retina signatures, and secure access devices.

16. The apparatus of Claim 14, wherein the encryption unit comprises full-disk encryption software.

17. The apparatus of Claim 11, wherein one of the non-volatile storage regions is adapted to store an operating system and data common to the first user and to the second user.

18. The apparatus of Claim 11, wherein one of the non-volatile storage regions is adapted to store user-specific data of the first user.

19. The apparatus of Claim 11, wherein one of the non-volatile storage regions is adapted to store user-specific data of the second user.

20. The apparatus of Claim 11, wherein the non-volatile storage regions are chosen from the group consisting of: volumes, disks, partitions, and folders/directories.

21. A computer program product comprising:

means for encrypting a plurality of non-volatile storage regions, each non-volatile storage region being encrypted using a different encryption key from a set of encryption keys;

means for making a first subset of the encryption keys available to a first user thereby granting the first user access to a corresponding first subset of non-volatile storage regions, the first subset of the encryption keys consisting of one, a plurality, or all of the encryption keys; and

means for making a second subset of the encryption keys available to a second user thereby granting the second user access to a corresponding second subset of non-volatile storage regions, the second subset consisting of one, a plurality, or all of the encryption keys.

22. The computer program product of Claim 21, further comprising:

means for generating a first private-public encryption key pair and a second private-public encryption key pair;

means for making the first private key available only to the first user and the second private key only to the second user; and

means for encrypting the first subset of the encryption keys using the first public encryption key and the second subset of the encryption keys using the second public encryption key.

23. The computer program product of Claim 22, further comprising:

means for storing the first private key and the second private key;

means for protecting access to the first private key with a first authentication token, the first authentication token being known only to the first user; and

means for protecting access to the second private key with a second authentication token, the second authentication token being known only to the second user.

24. The computer program product of Claim 23, further comprising:

means for requesting an authentication token from a user attempting to access one or more of the non-volatile storage regions;

means for authenticating the user, if the user's authentication token matches one of the authentication tokens used to protect access to one of the private keys;

means for decrypting, using the authenticated user's private key, a corresponding subset of encryption keys, in response to authenticating the user; and

means for decrypting a corresponding subset of non-volatile storage regions, thereby making the corresponding subset of non-volatile storage regions available to the authenticated user.

25. The computer program product of Claim 23, wherein the authentication tokens are selected from the group consisting of: passwords, fingerprints signatures, voice signatures, retina signatures, and secure access devices.

26. The computer program product of Claim 24, wherein the means for encrypting and the means for decrypting the plurality of non-volatile storage regions comprises full-disk encryption software.

27. The computer program product of Claim 21, wherein one of the non-volatile storage regions is adapted to store an

operating system and data common to the first user and the second user.

28. The computer program product of Claim 21, wherein one of the non-volatile storage regions is adapted to store user-specific data of the first user.

29. The computer program product of Claim 21, wherein one of the non-volatile storage regions is adapted to store user-specific data of the second user.

30. The computer program product of Claim 21, wherein the non-volatile storage regions are chosen from the group consisting of: volumes, disks, partitions, and folders/directories.